Identity Theft Prevention

The crime of identity theft is on the rise and has become a significant problem

Avoid Becoming a Victim of Identity Theft

To minimize the amount of information an identity thief can steal, do not carry extra credit cards, a Social Security card, birth certificate or passport in your wallet or purse, except when needed.

To reduce the amount of personal information that is in circulation consider the following:

- Remove your name from the marketing lists of the three major credit reporting bureaus, i.e., Equifax, Experian (formerly TRW) and Trans Union. This will limit the number of pre-approved offers of credit that you receive. These offers, if thrown away in the trash, are potential targets of identity thieves who will use them to order credit cards using your identity.

- Sign-up for the Direct Marketing Association Mail Preference Service and the Telephone Preference Service. By doing this, your name is added to computerized name deletion lists used by nationwide marketers.

- Have your name and address removed from telephone books and reverse directories.

- Install a locked mailbox at your residence or business to reduce mail theft or use a post office box.

- When you order new checks, do not have them sent to your home address. Instead, have them sent to a post office box or arrange to pick them up at your bank.

- When you pay bills, do not place the envelopes containing your checks in your home mailbox for the letter carrier to pick up. If stolen, your checks can be altered and cashed by identity thieves. It is best to mail your checks and other sensitive mail at the post office, rather than leave them in your home or neighborhood mailbox. Write checks with a fine-point permanent marker.

- Pay bills with an electronic bill payment service.

- Reduce the number of credit cards you actively use to a bare minimum. Carry only one or two credit cards in your wallet. Cancel all unused credit card accounts. Even though you do not use these accounts, account numbers are recorded in your credit report along with other data that can be used by identity thieves.

- Keep a list and/or photocopy of all your credit cards, account numbers, expiration dates and telephone numbers of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditors in case your credit cards are stolen. Do the same with your bank accounts.

- Never provide your credit card number or other personal information over the telephone, unless you have a trusted business relationship with the person or company and you have initiated the telephone call. Identity thieves have been known to call their victims with a fake story that goes something like this, “Today is your lucky day! You have been chosen by the ‘Jane and John Doe Sweepstakes Committee’ to receive a free trip to Europe. All we need is your credit card number and expiration date to verify you as the lucky winner.”

- Order your credit report once a year from each of the three major credit bureaus to check for inaccuracies and fraudulent use of your accounts. Make sure that you recognize every line of information established in your file.

- Always take credit card receipts with you. Never throw them in a public trash container.

- Watch the mail when you expect a new or reissued credit card to arrive. Contact the issuer if the card does not arrive.

- When creating a password or Personal Identification Number (PIN), do not use the last four digits of your Social Security number, date of birth, middle name, the name of your family pet, consecutive numbers or anything else that could easily be discovered by identity thieves.

- Ask your financial institution to add extra security protection to your account. Most will allow you to use an additional code (a number or word) when accessing your account. Do not use your mother’s maiden name, as that is all too easily obtained by identity thieves.

- Memorize all your passwords. Do not record them on anything in your wallet or purse.

- Protect your Social Security number. Release it only when absolutely necessary (tax forms, employment records, most banking, stock and property transactions). The Social Security number is the key to your credit and bank accounts and is a prime target of identity thieves.

- Because of the risk of fraud, do not have your Social Security number printed on your checks. Do not let merchants write your Social Security number on your checks.

- Order your Social Security Earnings and Benefits Statement once a year to check for fraud.

- Carefully review your credit card statements for unauthorized use.

- Do not throw pre-approved credit offers in the trash or in a recycling container without first shredding them. The discarded credit offers can be used by identity thieves to order credit cards in your name and to have the credit cards mailed to their address.

- Do the same with other sensitive information like credit card receipts. Home shredders can be purchased at many office supply stores.

- Demand financial institutions to adequately safeguard your data. Request a special password that only you will know. Memorize all passwords. Discourage your bank from using the last four digits of the Social Security number as the PIN they assign to customers.

- When you fill out loan applications, find out how the company disposes of them. If you are not convinced that they store them in locked files and/or shred them take your business elsewhere. Some car dealerships, department stores, car rental agencies and video stores have been known to be careless with customer applications. When you pay by credit card, ask the business how it stores and disposes of the transaction slip. Avoid paying by credit card if you think the business does not use adequate safeguards.

- Store your cancelled checks in a safe place. In the wrong hands, they can reveal a lot of information about you. Never permit your credit card number to be written on your checks.

- Any entity involved in handling personal information should train all its employees, from the top to the bottom, on responsible information-handling practices. Persuade the companies, government agencies and nonprofit agencies with which you are associated to adopt privacy policies and conduct privacy training.

If you become a victim of identity theft

- If you become the victim of identity theft, it is important to act immediately to stop the thief's further use of your identity. Unfortunately, at this time victims themselves are burdened with resolving the problem. It is important to act quickly and assertively to minimize the damage. In dealing with authorities and financial institutions, keep a log of all conversations, dates, names and telephone numbers. Note the time spent and any expenses incurred.

- Confirm conversations in writing. Provide your police report number to expedite reporting the crime. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.

- Sometimes victims of identity theft are wrongfully accused of crimes committed by an imposter. If a civil judgment has been entered in your name for actions taken by an imposter, contact the court where the judgment was entered and report that you are a victim of identity theft.

If you are wrongfully charged, contact the Virginia State Police and the FBI. Ask how to clear your name.

Also do the following

- Report the crime to local law enforcement. Give them as much documented evidence as possible. Obtain a copy of all police reports. Keep the telephone number of your fraud detective/investigator handy and give it to creditors and others who require verification of your case. Credit card companies, banks and insurance companies may require you to show the report in order to verify the crime. Some police and sheriff's departments have been known to refuse to write reports on such crimes. Be persistent!

- Immediately contact (by telephone and in writing) all creditors with whom your name has been used fraudulently. Obtain replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request." (This is better than "card lost or stolen," because when this statement is reported to credit reporting bureaus, it can be interpreted as blaming you for the loss.) Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

- If you have had checks stolen or bank accounts set up fraudulently, notify your bank. Report the fraud to check verification companies. Place stop payments on any outstanding checks about which you are unsure. Cancel your checking and savings accounts and obtain new account numbers. Ask the bank to issue you a secret password that must be used in every transaction (not your mother's maiden name). Write a form letter that can be mailed or faxed whenever you receive an inquiry about fraudulent checks written from your bank account. The letter should give a brief description of what happened, check numbers and check manufacturer (obtained from your bank), bank account number, case number (assigned by police or the law enforcement agency with jurisdiction), the name of the police or sheriff detective/investigator handling your case, and the name and telephone number of the customer service representative at your bank.

- The U.S. Secret Service has jurisdiction over financial fraud cases, but it usually does not investigate individual cases unless the dollar amount is high and/or you are one of many victims of a fraud ring. To interest the Secret Service in your case, you may want to ask the fraud department of the credit card companies and/or banks, as well as the police or sheriff's detective/investigator, to notify the particular Secret Service agent they work with regarding your case.

- Call the Social Security Administration to report fraudulent use of your Social Security number. Also, order a copy of your Social Security Earnings and Benefits Statement and check it for accuracy. As a last resort, you might want to change your number. The SSA will only change it if you fit their fraud victim criteria. Caution: This step should be reserved for only the most extreme situations. You must be sure to notify all credit grantors and credit reporting bureaus of your new Social Security number. The Social Security Administration has a fraud hotline to help victims. Call (800)-269-0271 or download more information about Social Security numbers and identity theft at www.ssa.gov/pubs/idtheft.htm.

- Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit credit or bank fraud against you. Notify the local Postal Inspector if you suspect mail theft. Theft of mail is a felony. Find out where fraudulent credit cards were sent. Notify the local Postmaster to have all mail forwarded in your name sent to your own address.

You also may need to talk with your mail carrier.

- If you have a passport, notify the passport office to be on the lookout for anyone ordering a new passport fraudulently.

- Call electrical, gas and water utilities. Alert them to the possibility that someone may attempt to open a new service using your identification.

- You may want to change your driver license number if someone is using your license as identification to pass bad checks. Call the Department of Motor Vehicles (DMV) to see if another license has been issued in your name. Place a fraud alert in your DMV records. Go to your local DMV office to request a new driver license number.

- Also, fill out a DMV complaint form to begin the fraud investigation process. Send supporting documents with the completed form to the nearest DMV investigation office. Be persistent!

- You may want to consult an attorney to determine legal action to take against creditors and/or credit bureaus if they are not cooperative in removing fraudulent entries from your credit report or if negligence is a factor. Call the local Bar Association to find an attorney who specializes in consumer law and the Fair Credit Reporting Act.

- Pay attention to your own mental health. Victims of identity theft often report a sense that they are blame. They often feel violated and powerless due to the fact that few; if any, of the authorities they have notified of the crime step forward to help them.

- Psychological counseling may help you deal with the stress and anxiety commonly experienced by victims. Discuss your situation with a trusted friend, spiritual advisor or counselor.

- Do not give-in and do not pay any bill or portion of a bill, which is the result of identity theft. Do not pay any checks, which were written and/or cashed fraudulently. Your credit rating should not be permanently affected, and no legal action should be taken against you. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but do not allow yourself to be coerced into paying fraudulent bills.

- Finally, speak with the detective investigating your case, he or she may be able to assist you in obtaining a fingerprint comparison if the suspect has ever been arrested or has used your name during an arrest. You

may be able to obtain information regarding any warrants connected to the arrest; this also may help in reestablishing your credit or obtaining a new Social Security number.

Credit Reporting Bureaus

- Contact credit reporting bureaus for names and telephone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit reporting bureaus to remove inquiries that have been generated due to the fraudulent access. You may also ask the credit reporting bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers).

- The nearest office of the Consumer Credit Counseling Service might be able to give you advice on removing fraudulent claims from your credit report.

- Immediately call the fraud units of the three credit reporting bureaus, i.e., Equifax (800-525-6285), Experian (888-397-3742; formerly TRW) and Trans Union (800-680-7289). Report the theft of your credit cards or numbers. Ask that your accounts be flagged. Also, add a victim's statement to your report, up to 100 words. ["My Identification has been used to apply for credit fraudulently. Contact me at (telephone number) to verify all applications."] Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary. Be aware that these measures may not entirely stop new fraudulent accounts from being opened by an imposter. Ask the credit bureaus in writing to provide you with free copies every few months so you can monitor your credit report.